JC14 Rec'd PCT/PTO 15 JAN 2002

FORM-PTO-1390 (Rev. 9-2001) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 032326-193

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5): Unassigned 10/031065

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR00/02009	12 July 2000	15 July 1999

TITLE OF INVENTION
METHOD FOR IMPROVING A RANDOM NUMBER GENERATOR TO MAKE IT MORE RESISTANT AGAINST ATTACKS BY CURRENT MEASURING

APPLICANT(S) FOR DO/EO/US
Jean-Sébastien CORON and David NACCACHE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☐ Other items or information:

21839

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Unassigned 10/031065	PCT/FR00/02009	032326-193

531 Rec'd PCT/PTO 15 JAN 2002

21. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,040.00 (960)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $890.00 (970)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $740.00 (958)		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) $710.00 (956)		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 890.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

Claims	Number Filed	Number Extra	Rate		
Total Claims	14 -20 =	-0-	X$18.00 (966)	$ -0-	
Independent Claims	4 -3 =	1	X$84.00 (964)	$ 84.00	
Multiple dependent claim(s) (if applicable)			+$280.00 (968)	$ -0-	
TOTAL OF ABOVE CALCULATIONS =				$ 974.00	
Reduction for 1/2 for filing by small entity, if applicable (see below).			+	$ -0-	-
SUBTOTAL =				$ 974.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)).			+	$ -0-	
TOTAL NATIONAL FEE =				$ -0-	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property			+	$ -0-	
TOTAL FEES ENCLOSED =				$ 974.00	
				Amount to be refunded:	$
				charged:	$

a. ☐ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 974.00 to cover the above fees is enclosed.

c. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

January 15, 2002
DATE

Patent
Attorney's Docket No. 032326-193

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Jean-Sébastien CORON et al	Group Art Unit: Unassigned
Application No.: Unassigned	Examiner: Unassigned
Filed: January 15, 2002	
For: METHOD FOR IMPROVING A RANDOM NUMBER GENERATOR TO MAKE IT MORE RESISTANT AGAINST ATTACKS BY CURRENT MEASURING	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title appearing on lines 1 and 2, insert the following:

--This disclosure is based upon French Application No. 99/09316, filed on July 15, 1999 and International Application No. PCT/FR00/02009, filed July 12, 2000, which was published on January 25, 2001 in a language other than English, the contents of which are incorporated herein by reference.

Background of the Invention--

Page 4, before line 28, insert the following heading:

--**Description of the Invention**--

Add the following Abstract:

--Two methods for random number generation are modified to make them more resistant to attacks by current measurements. The methods are particularly designed to be implemented in electronic devices such as smart cards, PCMCIA, badges, contactless cards or any other portable device. The DES algorithm is encrypted using a key K having a value D representing date information, to generate an integer variable I. For j ranging from 1 to m, the following steps are carried out: substituting s with s XOR I; introducing in the integer variable y the result of the encryption of s with the DES algorithm using the key K; introducing in x_j the result of y or s; substituting s with y XOR I; and introducing in s the result of the encryption of s with the DES algorithm using the key K. The sequence (x_1, x_2, x_m) is then restored in the output.--

IN THE CLAIMS:

Kindly replace claims 1-8, as follows.

1. (Amended) A method for generating random numbers using the Data Encryption Standard (DES) algorithm with a secret key K, said method taking as input a random integer s of size 64 bits, and an integer m, said method sending back as output m 64-bit random integers x_1, x_2, ..., x_m, said method comprising the following three steps:

1) With the DES algorithm and using the key K, encrypt a value D representing date data and put the result in an integer variable I;

2) For j in the range 1 to m:

2a) Replace s by s XOR I,

2b) Put in the integer variable y the result of the encryption of s with the DES algorithm using the key K,

2c) Put in x_j the result of y XOR s,

2d) Replace s with y XOR I,

2e) Put in s the result of the encryption of s with the DES algorithm using the secret key K; and

3) Return as output the succession $(x_1, x_2, \ldots, x_m)$.

2. (Amended) A method for generating random numbers, said method taking as input a random integer s of size 64 bits and an integer m, and sending back as output m 64-bit random integers $x_1, x_2, \ldots, x_m$, by using the Data Encryption Standard (DES) with a secret key K, an integer intermediate variable y, and a source S of quality deemed to be insufficient of random integers on 64 bits $x_1, x_2, \ldots, x_m$, said method comprising the following two steps:

1) For j in the range 1 to m:

1a) Generate an integer I by means of the source S,

1b) Replace s with s XOR I,

1c) Put in y the result of the encryption of s with the DES algorithm using the key K,

1d) Put in x_i the result of y XOR s,

1e) Replace s with y XOR I,

1f) Put in s the result of the encryption of s with the DES algorithm using the key K; and

2) Return as output the succession (x_1, x_2, ..., x_m).

3. (Amended) A handheld, wearable, or portable device that executes the following steps to generate m 64-bit random integers x_1, x_2, . . ., x_m:

1) With the DES algorithm and using a key K, encrypt a value D representing date data and put the result in an integer variable I;

2) For j in the range 1 to m:

2a) Replace a random integer s by s XOR I,

2b) Put in an integer variable y the result of the encryption of s with the DES algorithm using the key K,

2c) Put in x_j the result of y XOR s,

2d) Replace s with y XOR I,

2e) Put in s the result of th encryption of s with the DES algorithm using the secret key K; and

3) Return as output the succession (x_1, x_2, . . ., xm).

4. (Amended) An electronic device according to claim 3, wherein said device is a smart card.

5. (Amended) An electronic device according to claim 3, wherein said device is a contactless card.

6. (Amended) An electronic device according to claim 3, wherein said device is a Personal Computer Memory Card International Association (PCMCIA) card.

7. (Amended) An electronic device according to claim 3, wherein said device is a badge.

8. (Amended) An electronic device according to claim 3, wherein said device is a smart watch.

Add the following new claims.

9. (New) A handheld, wearable, or portable device that executes the following steps to generate m 64-bit random integers $x_1, x_2, \ldots, x_m$:

1) For j in the range 1 to m:

1a) Generate a 64-bit random integer I,

1b) Replace a 64-bit random integer s with s XOR I,

1c) Put in an integer variable y the result of the encryption of s with the DES algorithm using the key Y,

1d) Put in x_i the result of y XOR s,

1e) Replace s with y XOR I,

1f) Put in s the result of the encryption of s with the DES algorithm using the key K; and

2) Return as output the succession $(x_1, x_2, \ldots, x_m)$.

10. (New) An electronic device according to claim 9, wherein said device is a smart card.

11. (New) An electronic device according to claim 9, wherein said device is a contactless card.

12. (New) An electronic device according to claim 9, wherein said device is a Personal Computer Memory Card International Association (PCMCIA) card.

13. (New) An electronic device according to claim 9, wherein said device is a badge.

14. (New) An electronic device according to claim 9, wherein said device is a smart watch.

REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: January 15, 2002

Attachment to Preliminary Amendment dated January 15, 2002

Marked-up Claims 1-8

1. (Amended) A method for generating random numbers using the Data Encryption Standard (DES) algorithm with a secret key K [that must be used only in that algorithm], said method taking as input a random [and secret] integer s of size 64 bits, and an integer m, said method sending back as output m 64-bit random integers x_1, x_2, ..., x_m, said method [being characterized in that it comprises] comprising the following three steps:

2) With the DES algorithm and using the key K, encrypt a value D representing date data and put the result in an integer variable I[.];

3) For j in the range 1 to m:

2[)]a) Replace s by s XOR I[.],

2[)]b) Put in the integer variable y the result of the encryption of s with the DES algorithm using the key K[.],

2[)]c) Put in x_j the result of y XOR s[.],

2[)]d) Replace s with y XOR I[.],

2[)]e) Put in s the result of the encryption of s with the DES algorithm using the secret key K[.]; and

4) Return as output the succession (x_1, x_2, ..., x_m).

2. (Amended) A method for generating random numbers [making it possible to improve the quality of a random number generator whose quality is deemed to be insufficient], said method taking as input a random [and secret] integer s of size 64 bits and

Attachment to Preliminary Amendment dated January 15, 2002

Marked-up Claims 1-8

an integer m, and sending back as output m 64-bit random integers x_1, x_2, ..., x_m, [said method] by using the Data Encryption Standard (DES) with a secret key K [which must be used only in that algorithm], [said method using] an integer intermediate variable y, [said method using] and a source S of quality deemed to be insufficient of random integers on 64 bits x_1, x_2, ..., x_m, said method [being characterized in that it comprises] comprising the following two steps:

1) For j in the range 1 to m:

1[)]a) Generate an integer I by means of the source S[.],

1[)]b) Replace s with s XOR I[.],

1[)]c) Put in y the result of the encryption of s with the DES algorithm using the key K[.],

1[)]d) Put in x_i the result of y XOR s[.],

1[)]e) Replace s with y XOR I[.],

1[)]f) Put in s the result of the encryption of s with the DES algorithm using the key K[.]; and

2) Return as output the succession (x_1, x_2, ..., x_m).

3. (Amended) [An electronic device implementing the method according to claim 1 or 2, said device being characterized in that it is a] A handheld, wearable, or

Attachment to Preliminary Amendment dated January 15, 2002

Marked-up Claims 1-8

portable device that executes the following steps to generate m 64-bit random integers x_1, x_2, . . ., x_m:

1) With the DES algorithm and using a key K, encrypt a value D representing date data and put the result in an integer variable I;

2) For j in the range 1 to m:

2a) Replace a random integer s by s XOR I,

2b) Put in an integer variable y the result of the encryption of s with the DES algorithm using the key K,

2c) Put in x_j the result of y XOR s,

2d) Replace s with y XOR I,

2e) Put in s the result of th encryption of s with the DES algorithm using the secret key K; and

3) Return as output the succession (x_1, x_2, . . ., xm).

4. (Amended) An electronic device according to claim 3, [characterized in that it] wherein said device is a smart card.

5. (Amended) An electronic device according to claim 3, [characterized in that it] wherein said device is a contactless card.

Attachment to Preliminary Amendment dated January 15, 2002

Marked-up Claims 1-8

6. (Amended) An electronic device according to claim 3, [characterized in that it] wherein said device is a Personal Computer Memory Card International Association (PCMCIA) card.

7. (Amended) An electronic device according to claim 3, [characterized in that it] wherein said device is a badge.

8. (Amended) An electronic device according to claim 3, [characterized in that it] wherein said device is a smart watch.

METHOD FOR IMPROVING A RANDOM NUMBER GENERATOR TO MAKE IT MORE RESISTANT AGAINST ATTACKS BY CURRENT MEASURING

The present invention relates to an improvement in a method for generating random numbers or random sources, in particular sources developed in cryptographic systems such as random number generators on board smart cards.

In particular, it is intended to be implemented in testing and validating electronic devices of the following types: smart cards; Personal Computer Memory Card International Association (PCMCIA) cards; badges; contactless cards, or any other handheld, wearable, or portable device.

Most public-key cryptographic systems (also known as "asymmetric cryptography" systems) and most secret-key cryptographic systems (also known as "symmetric cryptography" systems) require secret random numbers to be drawn. It is essential for such random numbers

(which subsequently serve as keys) to be unpredictable *a priori*, and not to have any regular patterns enabling them to be found by exhaustive or improved exhaustive search strategies in which the most probable keys are looked for first.

It is possible to construct a random source on the basis of a function whose inverse is difficult to compute. Let f be such a function. It is possible to construct a random source by starting by selecting a random initialization variable s, and by applying the function f to the succession of values s, s+1, s+2, ... The output of the random source is defined as f(s),f(s+1),f(s+2),... As a function of the properties of the function f used, it can be preferable to keep only a few bits of the output f(s),f(s+1),f(s+2)...

A method for generating random numbers on the basis of a function whose inverse is difficult to compute is specified in ANSI Standard X9.17. That method uses the Data Encryption Standard (DES) algorithm with a secret key K that must be used only in that algorithm. The method for generating random numbers takes as input a random and secret integer s of size 64 bits, and an integer m, and sends back as output m 64-bit random integers x_1, x_2, ..., x_m. That method is characterized by the following three steps:

1) With the DES algorithm and using the key K, encrypt a value D representing date data and put the result in the integer variable I.

2) For j in the range 1 to m, execute the following steps:

2) a) Replace s by s XOR I.

2) b) Put in x_j the result of the encryption of s with the DES algorithm using the key K.

2) c) Replace s with x_j XOR I.

2) d) Put in s the result of the encryption of s with the DES algorithm using the secret key K.

3) Return as output the succession (x_1, x_2, ..., x_m).

It is possible to use this random number generator in an application for which the random number generator is already available, but is deemed to be of insufficient quality, e.g. a random number generator on board the microprocessor of a smart card. In which case, the above-described method is used to improve the quality of the random number generator. That method takes as input a random and secret integer s of size 64 bits and an integer m, and it sends back as output m 64-bit random integers x_1, x_2, ..., x_m. The method uses the Data Encryption Standard (DES) with a secret key K which must be used only in that algorithm. The method uses a source S of quality deemed to be insufficient of random integers on 64 bits. The method is characterized by the following three steps:

1) For j in the range 1 to m

1) a) Generate an integer I by means of the source S.

1) b) Replace s by s XOR I.

1) c) Put in x_j the result of the encryption of s with the DES algorithm using the key K.

1) d) Generating an integer I by means of the source S.

1) e) Replace s with x_j XOR I.

1) f) Put in s the result of the encryption s with the DES algorithm using the key K.

2) Return as output the succession (x_1, x_2, ..., x_m).

It has appeared that implementing a secret-key encryption algorithm (e.g. the DES algorithm) on a smart card is vulnerable to attacks consisting of differential analysis of current consumption or "Differential Power Analysis" (DPA) making it possible to discover the secret key. The principle of such DPA attacks is based on the fact that the power consumption of (i.e. the current consumed by) the microprocessor executing instructions varies depending on the item of data that is being manipulated. To discover the secret key, it is necessary for the input message or the output message of the encryption algorithm to be known.

The two above-described methods of generating random numbers are thus vulnerable to attacks of the DPA type. The random numbers sent back as output by those two methods are output messages from the encryption algorithm. On the basis of the power consumption of the smart card, it is thus possible to discover the encryption key K, and thus then to predict the output of the random number generator.

The method for the invention consists of a modification in the above-described methods of

generating random numbers so as to make them capable of withstanding DPA-type attacks.

The first modified method for generating random numbers uses the Data Encryption Standard (DES) algorithm with a secret key K that must be used only in that algorithm. It takes as input a random and secret integer s of size 64 bits, and an integer m, and sends back as output m 64-bit random integers x_1, x_2, ..., x_m. The method uses an intermediate integer variable y. The method is characterized by the following three steps:

1) With the DES algorithm and using the key K, encrypt a value D representing date data and put the result in an integer variable I.

2) For j in the range 1 to m, execute the following steps:

2) a) Replace s by s XOR I.

2) b) Put in the integer variable y the result of the encryption of s with the DES algorithm using the key K.

2) c) Put in x_j the result of y XOR s.

2) d) Replace s with y XOR I.

2) e) Put in s the result of the encryption of s with the DES algorithm using the secret key K.

3) Return as output the succession (x_1, x_2, ..., x_m).

In this improved method for generating random numbers, DPA-type current-measuring attack is impossible because the input and output messages of the DES encryption algorithm are not known.

The second improved method for generating random numbers is used to increase the quality of a random number generator whose quality is deemed to be insufficient. This method takes as input a random and secret integer s of size 64 bits and an integer m, and sends back as output m 64-bit random integers x_1, x_2, ..., x_m. The method uses the Data Encryption Standard (DES) with a secret key K which must be used only in that algorithm. The method uses a source S of quality deemed to be insufficient of random integers on 64 bits. The method is characterized by the following two steps:

1) For j in the range 1 to m:

1) a) Generate an integer I by means of the source S.

1) b) Replace s with s XOR I.

1) c) Put in y the result of the encryption of s with the DES algorithm using the key K.

1) d) Put in x_i the result of y XOR s.

1) e) Replace s with y XOR I.

1) f) Put in s the result of the encryption s with the DES algorithm using the key K.

2) Return as output the succession (x_1, x_2, ..., x_m).

In this improved method for generating random numbers, DPA-type current-measuring attack is impossible because the input and output messages of the DES encryption algorithm are not known.

Both of the preceding methods of generating random numbers thus make it possible to obtain a random number

generator that withstands DPA-type current-measuring attacks.

CLAIMS

1/ A method for generating random numbers using the Data Encryption Standard (DES) algorithm with a secret key K that must be used only in that algorithm, said method taking as input a random and secret integer s of size 64 bits, and an integer m, said method sending back as output m 64-bit random integers x_1, x_2, ..., x_m, said method being characterized in that it comprises the following three steps:

1) With the DES algorithm and using the key K, encrypt a value D representing date data and put the result in an integer variable I.

2) For j in the range 1 to m:

2) a) Replace s by s XOR I.

2) b) Put in the integer variable y the result of the encryption of s with the DES algorithm using the key K.

2) c) Put in x_j the result of y XOR s.

2) d) Replace s with y XOR I.

2) e) Put in s the result of the encryption of s with the DES algorithm using the secret key K.

3) Return as output the succession (x_1, x_2, ..., x_m).

2/ A method for generating random numbers making it possible to improve the quality of a random number generator whose quality is deemed to be insufficient, said method taking as input a random and secret integer s of size 64 bits and an integer m, and sending back as output m 64-bit random integers x_1, x_2, ..., x_m, said

method using the Data Encryption Standard (DES) with a secret key K which must be used only in that algorithm, said method using an integer intermediate variable y, said method using a source S of quality deemed to be insufficient of random integers on 64 bits x_1, x_2, ..., x_m, said method being characterized in that it comprises the following two steps:

1) For j in the range 1 to m:

1) a) Generate an integer I by means of the source S.

1) b) Replace s with s XOR I.

1) c) Put in y the result of the encryption of s with the DES algorithm using the key K.

1) d) Put in x_i the result of y XOR s.

1) e) Replace s with y XOR I.

1) f) Put in s the result of the encryption s with the DES algorithm using the key K.

2) Return as output the succession (x_1, x_2, ..., x_m).

3/ An electronic device implementing the method according to claim 1 or 2, said device being characterized in that it is a handheld, wearable, or portable device.

4/ An electronic device according to claim 3, characterized in that it is a smart card.

5/ An electronic device according to claim 3, characterized in that it is a contactless card.

6/ An electronic device according to claim 3, characterized in that it is a Personal Computer Memory Card International Association (PCMCIA) card.

7/ An electronic device according to claim 3, characterized in that it is a badge.

8/ An electronic device according to claim 3, characterized in that it is a smart watch.

032326-193
Attorney's Docket No.

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR IMPROVING A RANDOM NUMBER GENERATOR TO MAKE IT MORE RESISTANT AGAINST ATTACKS BY CURRENT MEASURING

the specification of which **(check only one item below)**:

☒ is attached hereto.

☐ was filed as United States Patent application
Number _____ on _____
and was amended on _____ (if applicable).

☒ was filed as PCT International application
Number PCT/FR00/02009 on 12 July 2000
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(d), 172 or 365 of any foreign application(s) for patent or inventor's certificate or of any international (PCT) application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international (PCT) application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §§119(a)-(d), 172 or 365:			
COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §§119, 172 or 365
France	99/09316	15 July 1999	☒Yes ☐No

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the U.S. Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	Eric H. Weisblatt	30,505	Bruce T. Wieder	33,815
Robert S. Swecker	19,885	James W. Peterson	26,057	Todd R. Walters	34,040
Platon N. Mandros	22,124	Teresa Stanek Rea	30,427	Ronni S. Jillions	31,979
Benton S. Duffett, Jr.	22,030	Robert E. Krebs	25,885	Harold R. Brown III	36,341
Norman H. Stepno	22,716	William C. Rowland	30,888	Allen R. Baum	36,086
Ronald L. Grudziecki	24,970	T. Gene Dillahunty	25,423	Brian P. O'Shaughnessy	32,747
Frederick G. Michaud, Jr.	26,003	Patrick C. Keane	32,858	Kenneth B. Leffler	36,075
Alan E. Kopecki	25,813	B. Jefferson Boggs, Jr.	32,344	Fred W. Hathaway	32,236
Regis E. Slutter	26,999	William H. Benz	25,952	Wendi L. Weinstein	34,456
Samuel C. Miller, III	27,360	Peter K. Skiff	31,917	Mary Ann Dillahunty	34,576
Robert G. Mukai	28,531	Richard J. McGrath	29,195	Donna M. Meuth	36,607
George A. Hovanec, Jr.	28,223	Matthew L. Schneider	32,814	Mark R. Kresloff	42,766
James A. LaBarre	28,632	Michael G. Savage	32,596		
E. Joseph Gess	28,510	Gerald F. Swiss	30,113		
R. Danny Huntington	27,903	Charles F. Wieland III	33,096		

21839

and: _____

Address all correspondence to:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

21839

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST INVENTOR	Jean-Sebastien CORON
Signature	
Date	21/02/2002
Residence (City, State, Country)	Paris, France
Citizenship	French
Mailing Address	4, rue Leon de Lagrange, F-75015, Paris, France
City, State, ZIP, Country	F-75015, Paris, France
FULL NAME SECOND INVENTOR, IF ANY	David NACCACHE
Signature	
Date	31/1/02
Residence (City, State, Country)	Paris, France
Citizenship	French
Mailing Address	7, rue, Chaptal, F-75009, Paris, France
City, State, ZIP, Country	F-75009, Paris, France